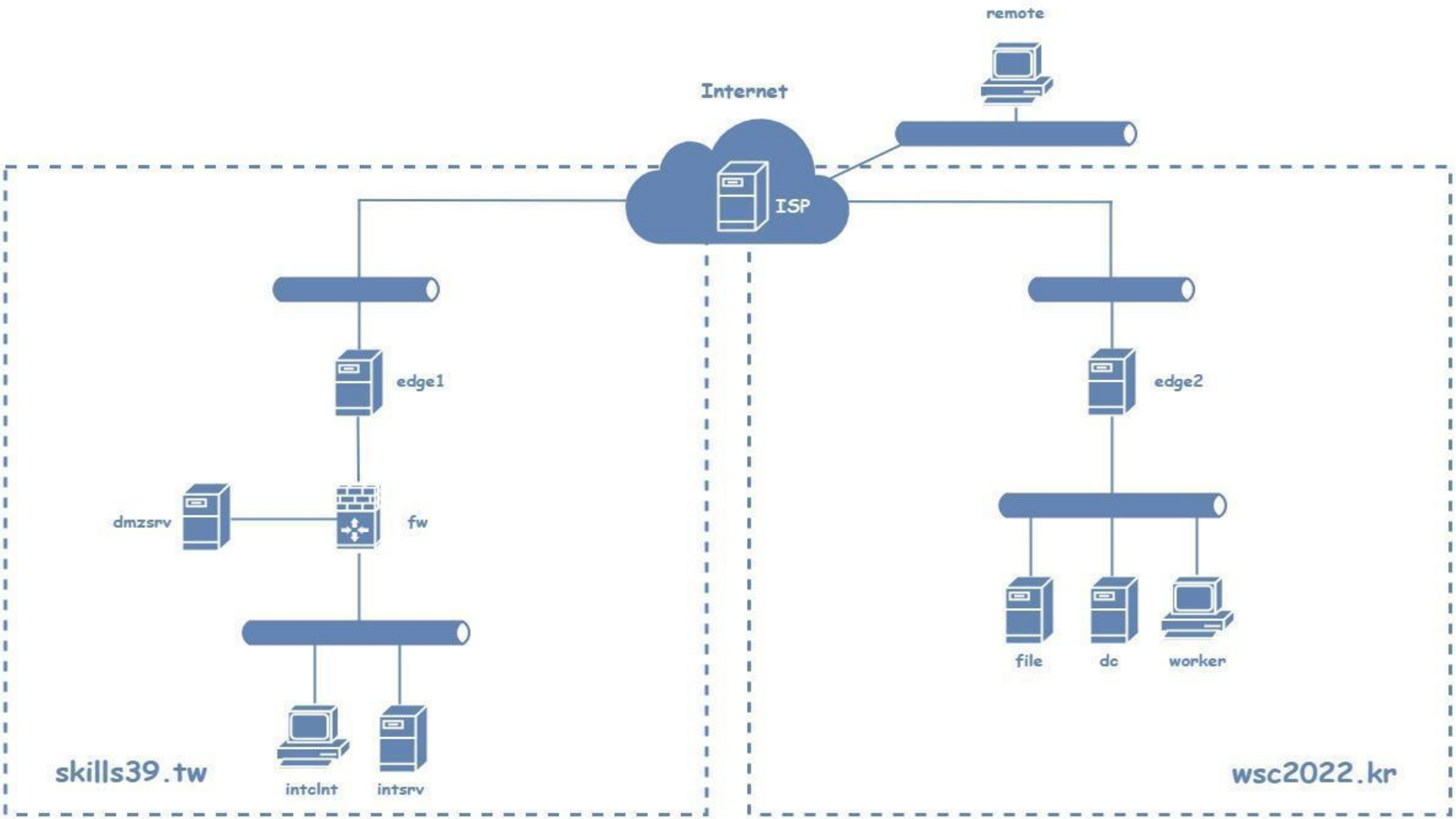
第五十二屆 全國技能競賽 資訊與網路技術

- 本競賽為固定式起訖時間，請選手自行掌握工作流程，並依據試題敘述完成要求。
- 如在比賽過程中有任何疑問，或題意描述不清楚，請立即向裁判反應。
- 工作項目中須設定密碼之處，若試題未明確指定，則一律使用 Skills39
- 評分時，將盡可能採用功能測試，項目之區隔以評分表所列為主，個別項目完全符合試題之敘述即得分，無部份給分。
- 除了必須以檢視設定值的方式進行評分的項目外，所有面向用戶的服務一律由用戶端系統進行功能測試，否則該項目不予計分

Network Diagram



第 1 站

基礎環境建設

- 將 ISP、edge1、edge2 組態為路由器，使 Internet 的主機能夠互相存取
- 將 fw 組態為路由器，使 skills39.tw 內部主機可正常通訊
- 於 edge1、edge2 設定 NAT，並使 skills39.tw、wsc2022.kr 內部主機可以存取 Internet
- 於 edge1、edge2 設定 GRE Tunnel，使 skills39.tw、wsc2022.kr 能夠互相存取

(如無法建立 GRE、選手可用另外的方式建立互通性，但請不要破壞原有的網路架構)

Active Directory

- 於 dc 上建立 ADDS，網域名稱為: wsc2022.kr，並依附表新增使用者及群組、組織單位
- 為所有使用者建立 home drive，路徑為 \\file\homes\%username%，並自動掛載至每個使用者的 H: 下
- 為所有使用者建立 roaming profile，路徑為 \\file\profiles\%username%
- 將 file 進入此網域並提升至 Domain Controller (No Global Catalog)

Group Policy

- 從 worker 主機登入將不顯示首次登入動畫
- Managers 群組的使用者登入時，使用 KR_USERS 範本自動註冊憑證
- 自動掛載群組資料夾至 G 槽

第 2 站

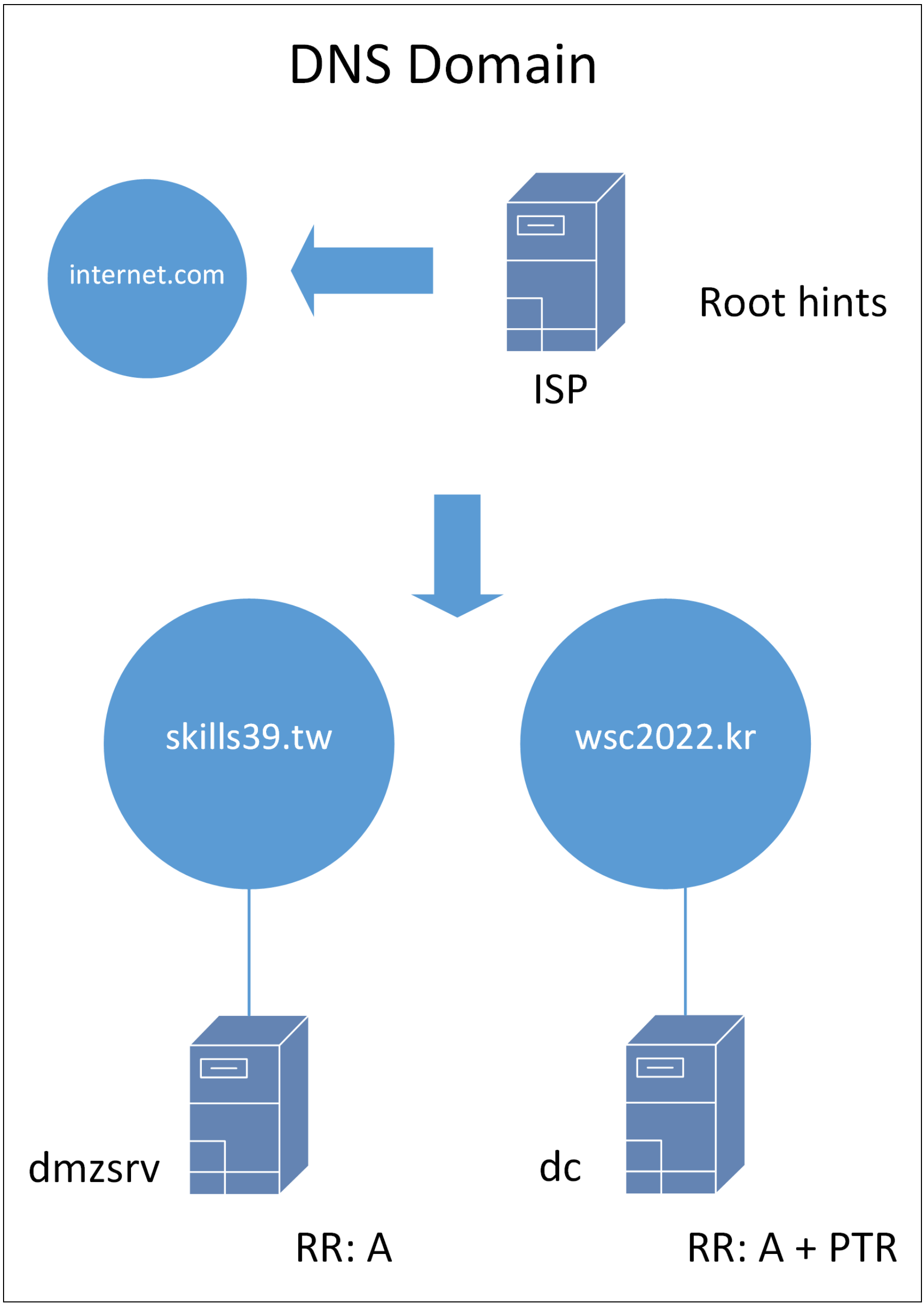
DNS

- 於 intsrv 設定 DNS，並做為 skills39.tw 的內部 Name Server
  - 為 skills39.tw 內部所有伺服器建立 A、PTR 紀錄
  - 依照服務的需求，建立適當的 CNAME 紀錄
  - 將 wsc2022.kr 的紀錄查詢轉交給 dc 查詢
  - 將 Root Hint 設為 ISP
  - 配合 edge1，允許 edge1 自動更新自身的資源紀錄

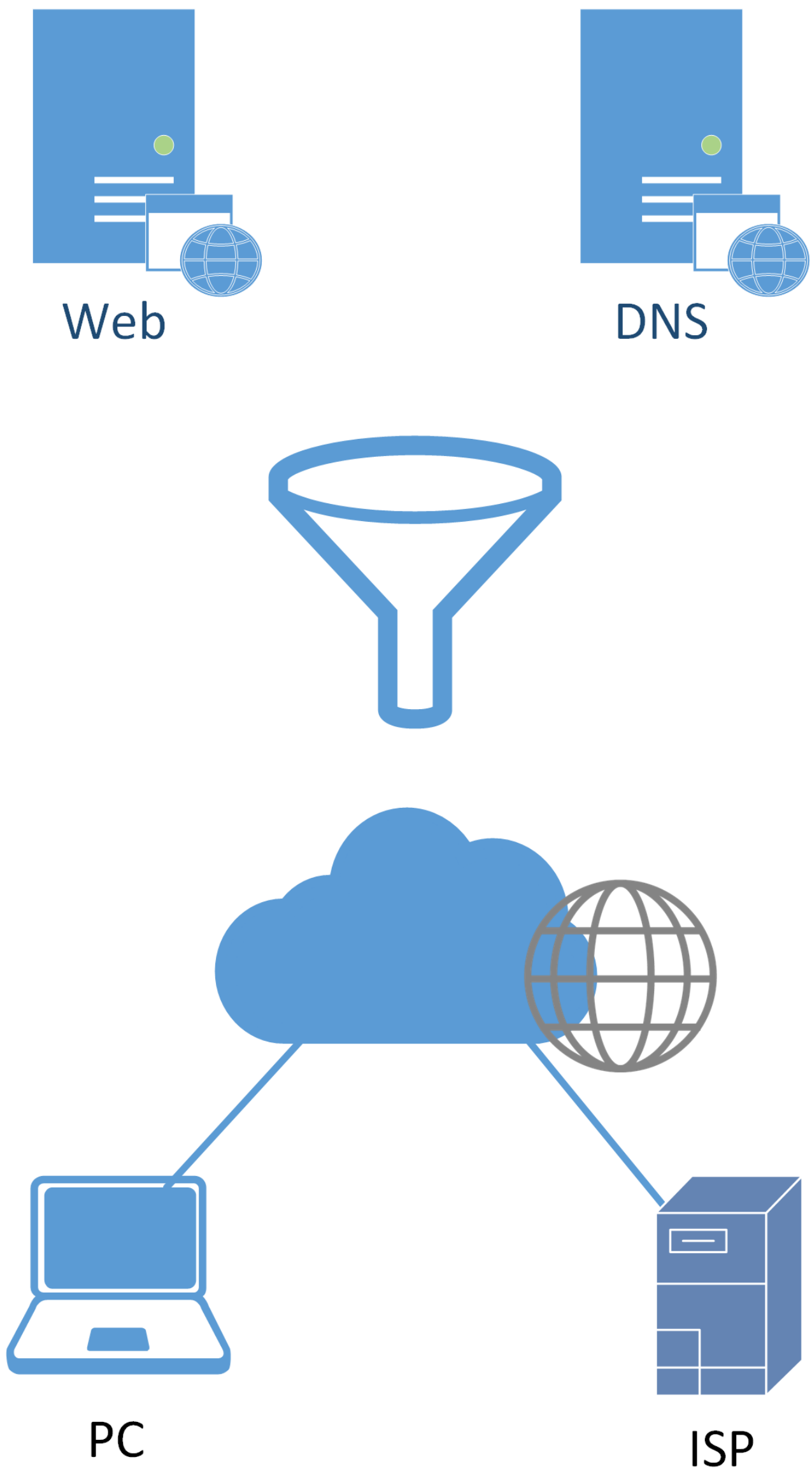
- 於 dmzsrv 設定 DNS，並做為 skills39.tw 的外部 Name Server
  - 建立適當的 A 紀錄
  - 依照服務的需求，建立適當的 CNAME 紀錄

- 於 dc 設定 DNS，同時做為 wsc2022.kr 的內部及外部 Name Server
  (請避免內部會查詢到外部的紀錄，反之亦然)
  - 為 wsc2022.kr 內部所有伺服器建立 A、PTR 紀錄
  - 為 wsc2022.kr 外部建立適當的 A 紀錄
  - 內部及外部都依照服務的需求，建立適當的 CNAME 紀錄
  - 將 skills39.tw 的紀錄查詢轉交給 intsrv
  - 將 Root Hint 設為 ISP

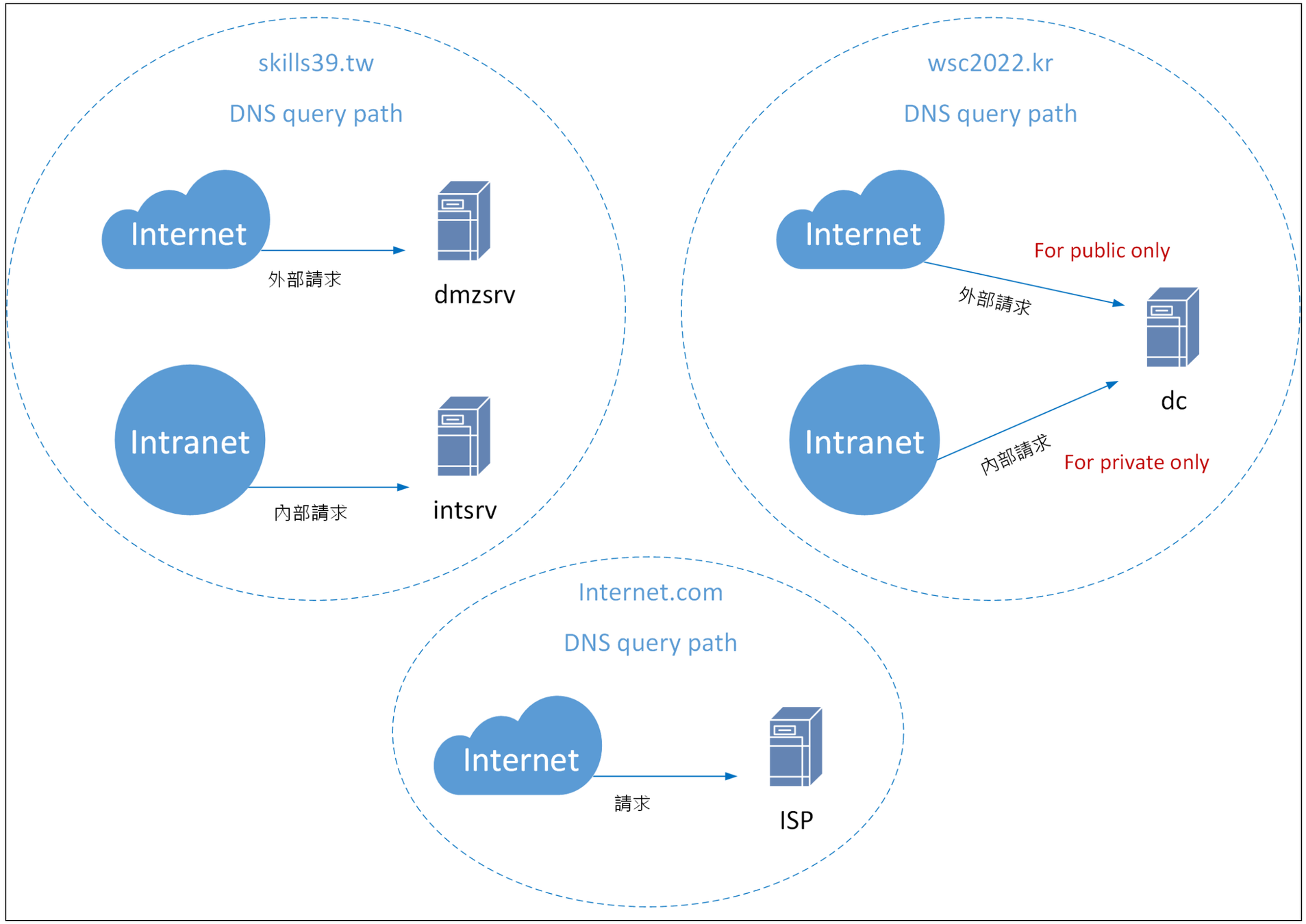
- 於 ISP 設定 DNS，做為 internet.com 的 Name Server
  - 為 internet.com 的所有伺服器建立 A 紀錄
  - 依照服務的需求，建立適當的 CNAME 紀錄
  - 提供 Microsoft NCSI，供所有 Windows 系統進行 Internet 檢測
  (Hint: 請參考 HKLM\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet)
  - 設定子網域授權，讓 internet 使用者可以查詢 skills39.tw、wsc2022.kr 的網域紀錄


DNS Domain
internet.com
ISP
Root hints
skills39.tw
wsc2022.kr
dmzsrv
dc
RR: A
RR: A + PTR

Microsoft NCSI



DNS Policy


skills39.tw
DNS query path
Internet
外部請求
dmzsrv
Intranet
內部請求
intsrv
wsc2022.kr
DNS query path
Internet
For public only
外部請求
dc
Intranet
內部請求
For private only
Internet.com
DNS query path
Internet
請求
ISP

第 3 站

DHCP

- 於 edge1 設定 DHCP，提供 skills39.tw 網域的內部 IP 資訊配發
  - 提供範圍為 192.168.1.100 - 199
  - 依照題目需求設定適當的 Options
  - A 與 PTR 紀錄將可自動更新至 intsrv

- 於 edge2 設定 DHCP 提供 wsc2022.kr 網域的內部 IP 資訊配發
  - 提供範圍為 172.16.1.100 – 199
  - 依照題目需求設定適當的 Options

- 於 fw 設定 DHCP Relay Agent，使 skills39.tw 內部主機能成功向 edge1 取得內部 IP 資訊

Web

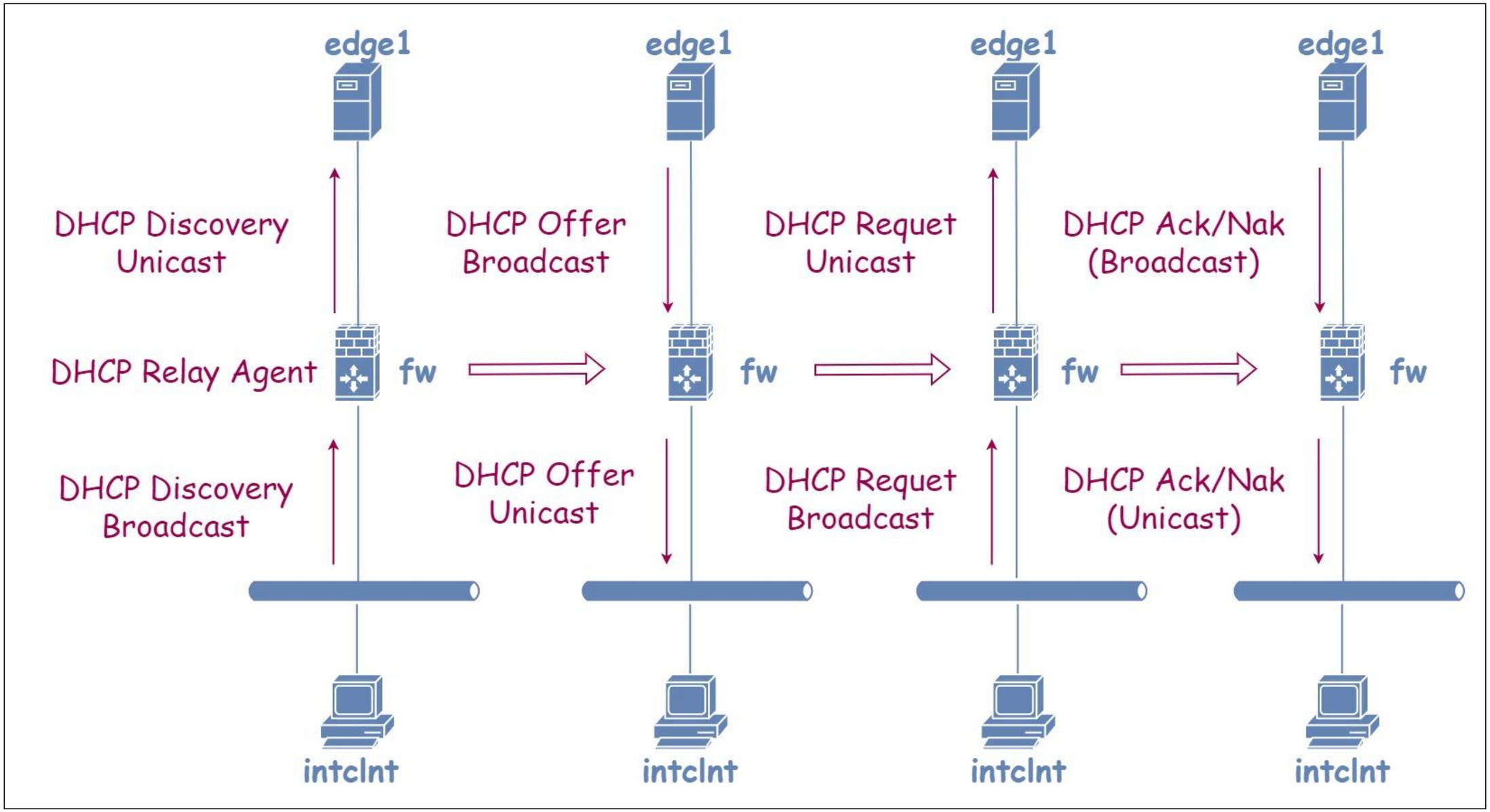
- 於 dmzsrv 設定 Web，提供 https://www.skills39.tw 站台
  - 憑證使用 WSC2022-KR-CA 進行簽屬
  - 建立 https://www.skills39.tw/wsc2022/，存取時使用 wsc2022.kr 網域的使用者進行驗證，並僅允許 Managers 群組。
  - 為首頁及 /wsc2022/ 建立簡單的測試頁面

- 於 dc 設定 Web，提供 https://www.wsc2022.kr 站台
  - 網頁根目錄為 C:\www\
  - 憑證使用 WSC2022-KR-CA 進行簽屬
  - 建立 https://www.wsc2022.kr/managers/ ，並啟用 Client Certificate 驗證
  - 為首頁及 managers 建立簡單的測試頁面

- 於 ISP 設定 Web，並依照以下提供所需之站台:
  - 提供 https://www.internet.com 站台，憑證使用自簽屬(self-signed)憑證
  - 提供 Microsoft NCSI 所需之網站，以利於 Windows 系統進行 Internet 測試

  (Hint: 請參考 HKLM\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet)

DHCP Relay


edge1
edge1
edge1
edge1
DHCP Discovery
Unicast
DHCP Offer
Broadcast
DHCP Requet
Unicast
DHCP Ack/Nak
(Broadcast)
DHCP Relay Agent
fw
fw
fw
fw
DHCP Discovery
Broadcast
DHCP Offer
Unicast
DHCP Requet
Broadcast
DHCP Ack/Nak
(Unicast)
intclnt
intclnt
intclnt
intclnt

第 4 站

Certificate Authority

- 於 dc 設定 ADCS，做為 wsc2022.kr 網域內部的企業 Root CA
  - Subject-Name 為 "CN=WSC2022-KR-CA"
  - 提供 CDP 以檢查憑證註銷，URL 為: http://dc.wsc2022.kr/certenroll/WSC2022-KR-CA.crl
  - 提供 AIA，URL 為: http://dc.wsc2022.kr/certenroll/WSC2022-KR-CA.crt
  - 建立 KR_USERS 憑證範本，提供給網域內的使用者

File Service

- 加兩顆硬碟到 Storage Pools，採用 RAID1，格式化為支援加密(EFS)的檔案系統並掛載至 V:\
- 於 file 建立共享資料夾 "WSC"
  - 本機路徑為 V:\WSC\
  - 建立三個子資料夾 Managers、Competitors、Visitors，做為 wsc2022.kr 網域內之群組資料夾
  - 三個子資料夾應對沒有權限的使用者進行隱藏(e.g. Manager 群組無法存取 Competitors 的資料夾)
- 於 file 建立共享資料夾 "Resource"
  - 此資料夾僅允許 Managers、Competitors 群組內的使用者存取
- 配合 AD 的需求建立 home drive、roaming profile
  - 所有使用者不可在 home drive 存放可執行檔案(e.g. exe、bat、cmd ..) 並限制存放容量上限為 100MB

Client Configuration

- 將 worker、inclnt 加入 wsc2022.kr 網域，且存取有 TLS/SSL 相關服務，不可跳出憑證錯誤訊息
- remote 瀏覽有關於 skills39.tw、wsc2022.kr、internet.com 之 HTTPS 網頁，不可跳出錯誤訊息

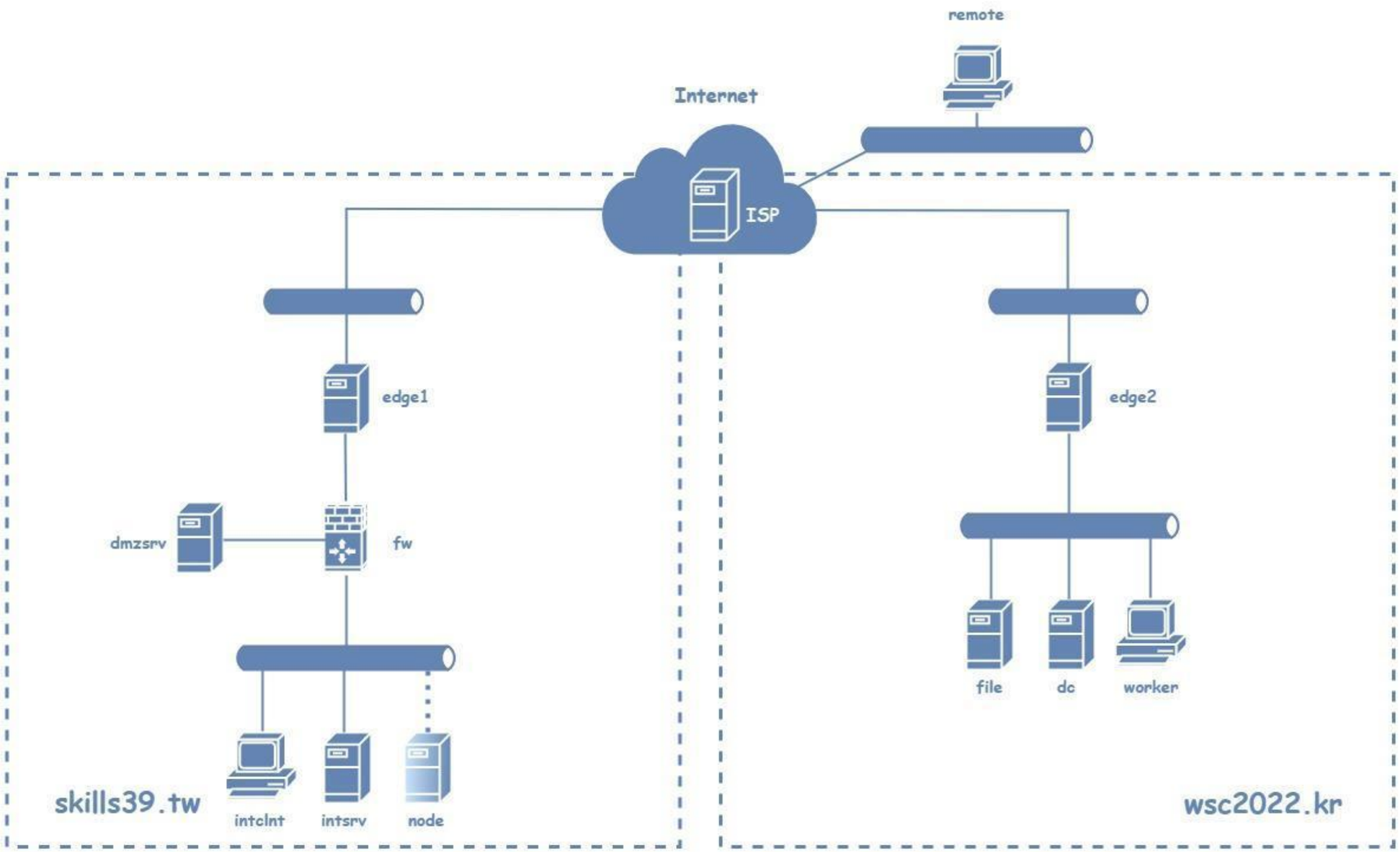
附錄 A、主機、網路相關設定

Hostname	OS	Interface	IP Address	Default Gateway
ISP	Debian 11	eth0	210.103.5.254/25	
		eth1	210.103.5.62/26	
		eth2	210.103.5.126/26	
edge1	Debian 11	eth0	10.1.1.2/30	210.103.5.62
		eth1	210.103.5.1/26	
		Tun0	10.2.1.1/30	
fw	Debian 11	eth0	10.1.1.1/30	10.1.1.2
		eth1	192.168.1.254/24	
		dmz	192.168.2.254/24	
Intsrv	Debian 11	eth0	192.168.1.1/24	192.168.1.254
dmzsrv	Debian 11	eth0	192.168.2.1/24	192.168.2.254
edge2	Windows Server 2019	Ethernet0	172.16.1.254/24	210.103.5.62
		Ethernet1	210.103.5.65/26	
		Tun0	10.2.1.2/30	
dc	Windows Server 2019	Ethernet0	172.16.1.1/24	172.16.1.254
file	Windows Server 2019	Ethernet0	172.16.1.2/24	172.16.1.254
worker	Windows 10	Ethernet	DHCP	
remote	Windows 10	Ethernet	210.103.5.210/25	210.103.5.254
Intclnt	Windows 10	Ethernet	DHCP	

附錄 B、Active Directory 使用者與群組

OU	Username	Group	Password
Managers	M01- M10	Managers	Skills39
Competitors	C01-C90	Competitors	
Visitors	V01–V100	Visitors	

Network


remote
Internet
ISP
edge1
edge2
dmzsrv
fw
file
dc
worker
intclnt
intsrv
node
skills39.tw
wsc2022.kr

第 5 站

Ansible

- 使用 intsrv 主機控制 node 主機，並建立資料夾 /playbooks
  - 評分時將會透過 “ansible-playbook <playbookname>.yml ” 進行測試
  - node 主機 VMnet 設定及登入資訊如附錄 C，評分前 node 主機會使用 OVA 重新匯入
  - 所有 playbook 都應位於此目錄的根目錄，您可以自行在此目錄中增加新的資料夾/檔案來運作 playbook
  - 在第二次運作 playbook 後，所有任務應該都只有兩種狀態： “ok” 或 “skipped”
- ping
  - 建立一個名稱為 1-ping.yml 的 playbook，使用 ansible 內建的 ping 模組檢測 node 主機的活躍狀態，成功連線時，請顯示 pong 訊息，如下圖

```
TASK [ping] ************************
ok: [node]

TASK [debug] ***********************
ok: [node] => {
    "msg": "pong"
}

PLAY RECAP *************************
node                       : ok=2
0    ignored=0
```

- SNMP
  - 建立一個名稱為 2-snmp.yml 的 playbook
  - 為 Linux 主機，依題目敘述設定 SNMP (啟用服務、設定驗證 ....)

第 6 站

Ansible

- Web
  - 建立名稱為 3-web.yml 的 playbook 以設置下列網頁服務：
    - 安裝網頁伺服器 (可以使用任何熟悉的套件)
    - 執行中要求輸入 webport，作為網站監聽 port
    - 執行中要求輸入 webcolor ，作為網站首頁內容的顏色
    - 執行中要求輸入 content ，作為網站首頁內容
    - 網頁語法如下：

      content

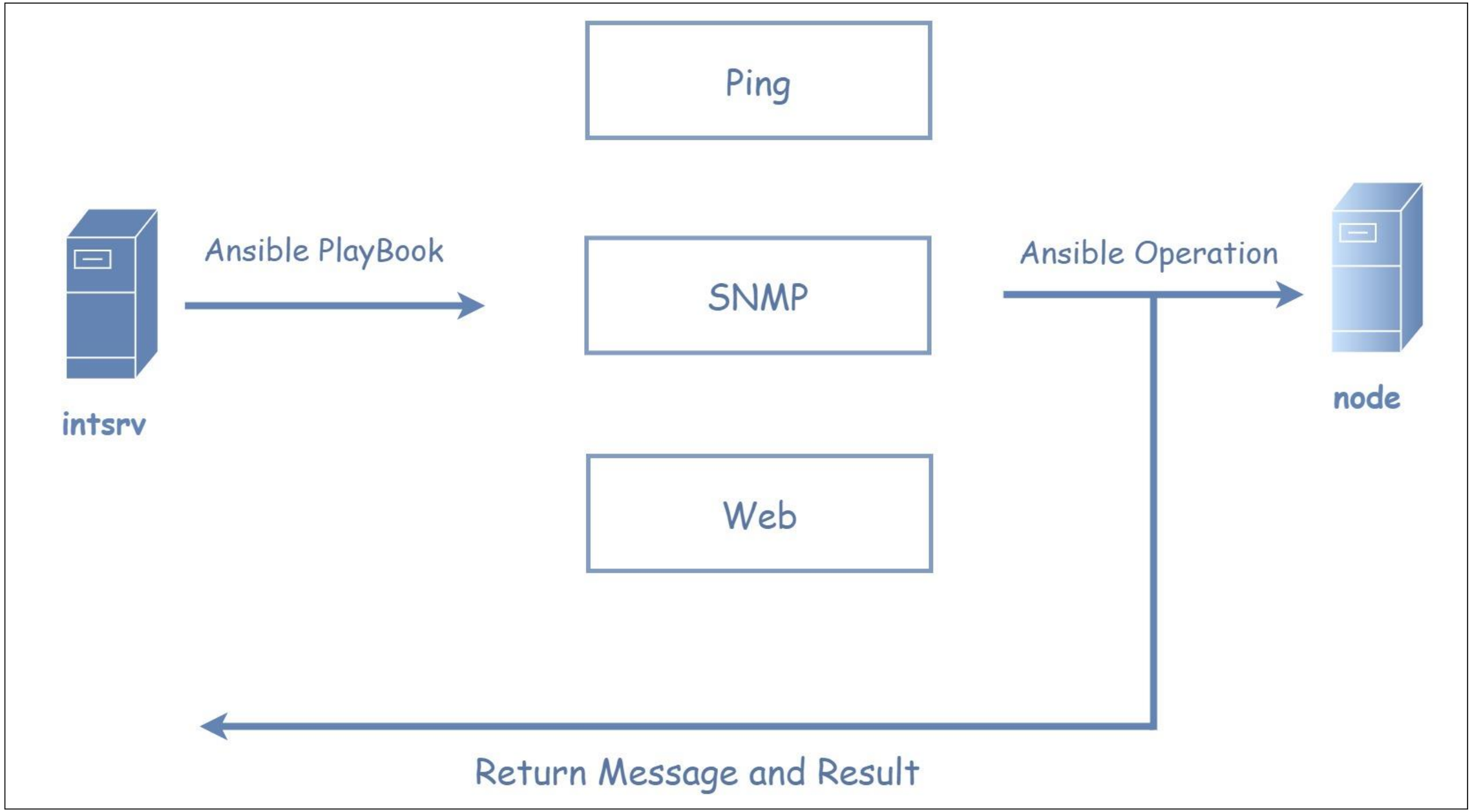
    - 執行輸入畫面：

      ```
      [redacted] /playbooks# ansible-playbook 3-web.yml
      Enter webport: 81
      Enter webcolor: blue
      Enter content: Hello From Ansible!
      ```

    - 網頁 HTML：

      Hello From Ansible!

Ansible


Ping
Ansible PlayBook
SNMP
Ansible Operation
intsrv
node
Web
Return Message and Result

第 7 站

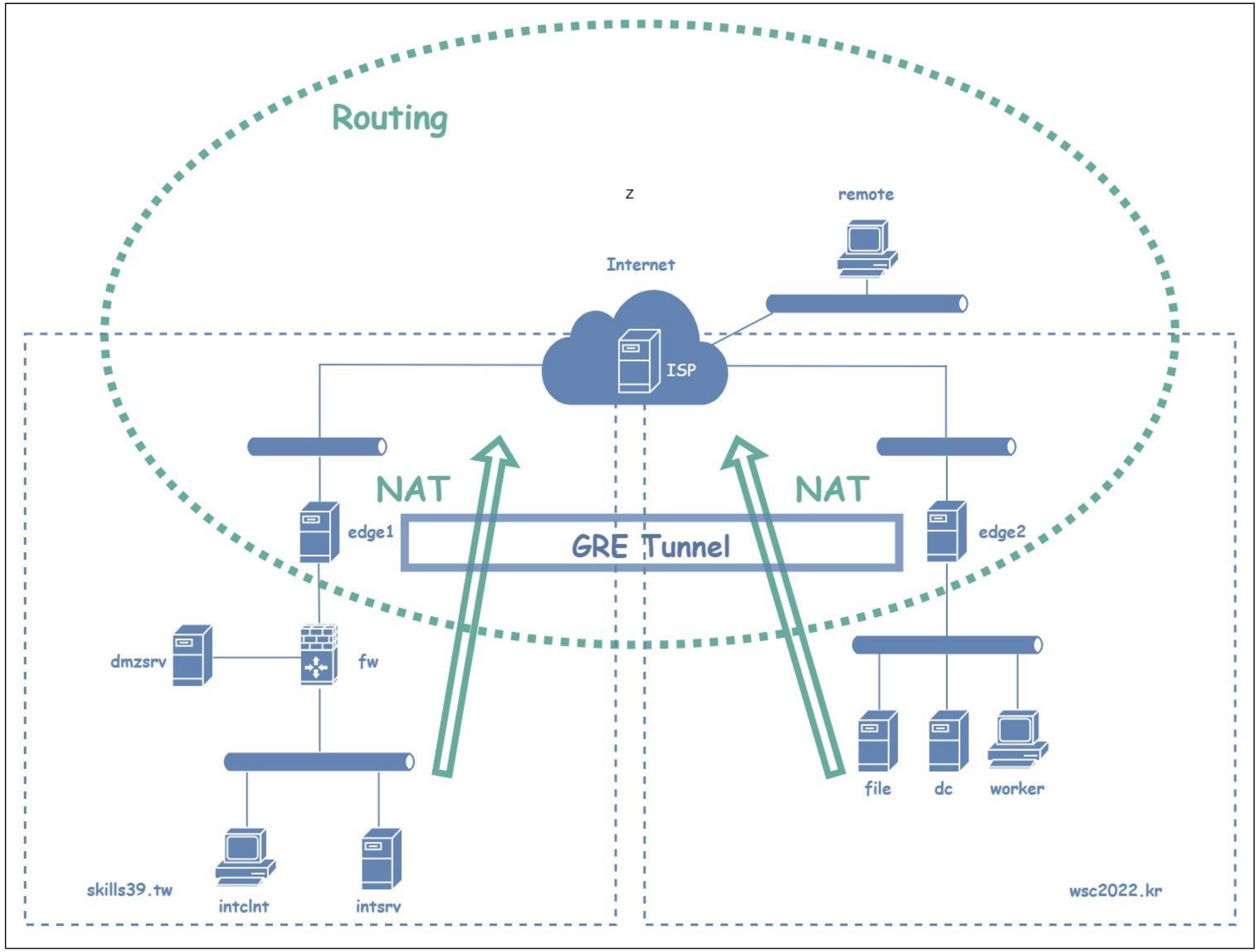
Remote Access VPN

- 於 fw 設定 OpenVPN
  - 使用 wsc2022.kr 網域的使用者進行資訊
  - 使用 vpn.skills39.tw 做為連接 VPN 的 Destination，憑證將使用 WSC2022-KR-CA 進行簽屬
  - 提供 192.168.3.0/24 網段給 VPN Client
  - 確保 VPN Client 可以連接至 dc

- 於 remote 設定 OpenVPN Client
  - 安裝 OpenVPN 的 Client 程式並進行設定
  - 預先設定 Profile，其名稱為 WSC

Firewall

- 於 fw 設定 Iptables
  - INPUT、FORWARD 請預設為 DROP
  - 允許 intsrv 與 dc 所在的內網相互存取
  - 禁止 dmzsrv 發起任何主動存取; 往 dmzsrv 的流量，僅允許服務所需的必要流量
  - 來自 Internet 網路到 dmzsrv 的流量，僅允許服務所需的流量
  - 此主機將能 ping 到任何主機


Routing
z
remote
Internet
ISP
NAT
NAT
edge1
GRE Tunnel
edge2
dmzsrv
fw
file
dc
worker
skills39.tw
intclnt
intsrv
wsc2022.kr

第 8 站

增強環境建設

- 將 edge1、edge2 之間的 GRE Tunnel，使用 IPsec 進行加密，並使用 Pre-Shared key 進行驗證

Monitoring

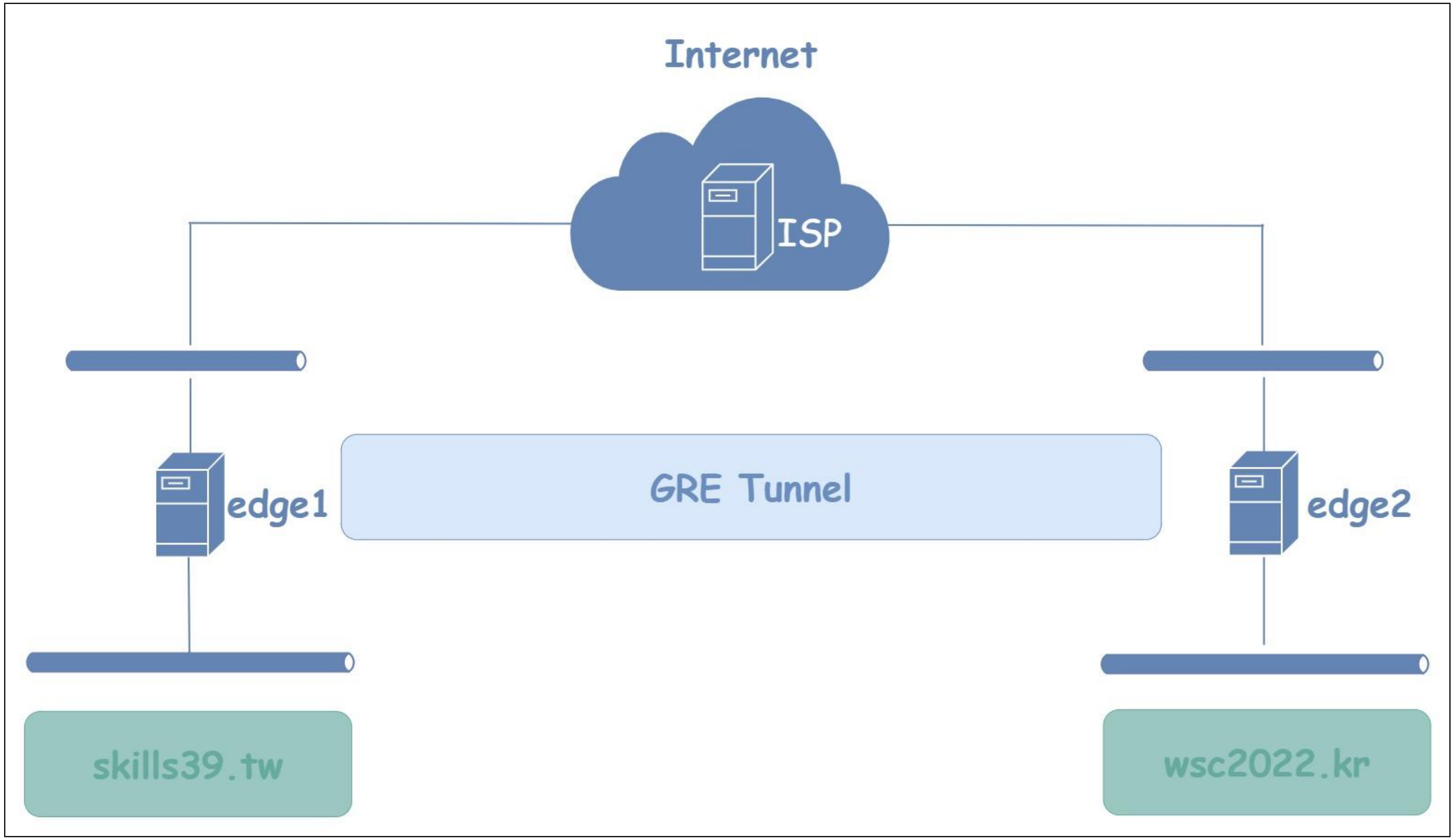
- 於 dc、intsrv 上設定 SNMP Agent
  - 設定版本為 SNMPv2，Community 為 "public"

- 於 dmzsrv 上設定 Cacti
  - 使用 http://monitor.skills39.tw/monitor 進行存取
  - 管理者密碼為 "Skill39##"
  - 監控 intsrv、dc 的所有網路介面的流量並生成圖表
  - 為每一台主機建立不同的 Tree

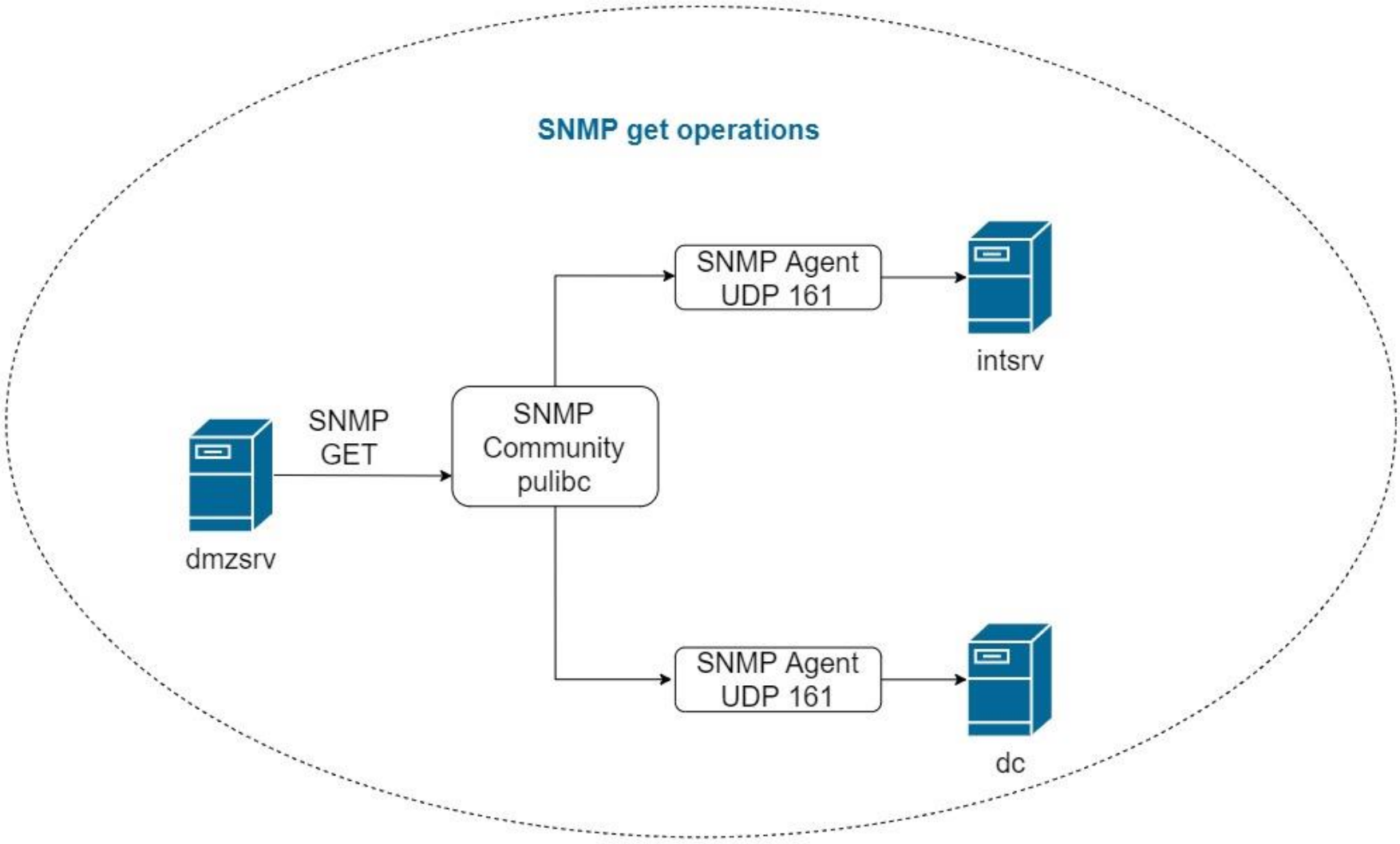
附錄 C、node 主機登入資訊

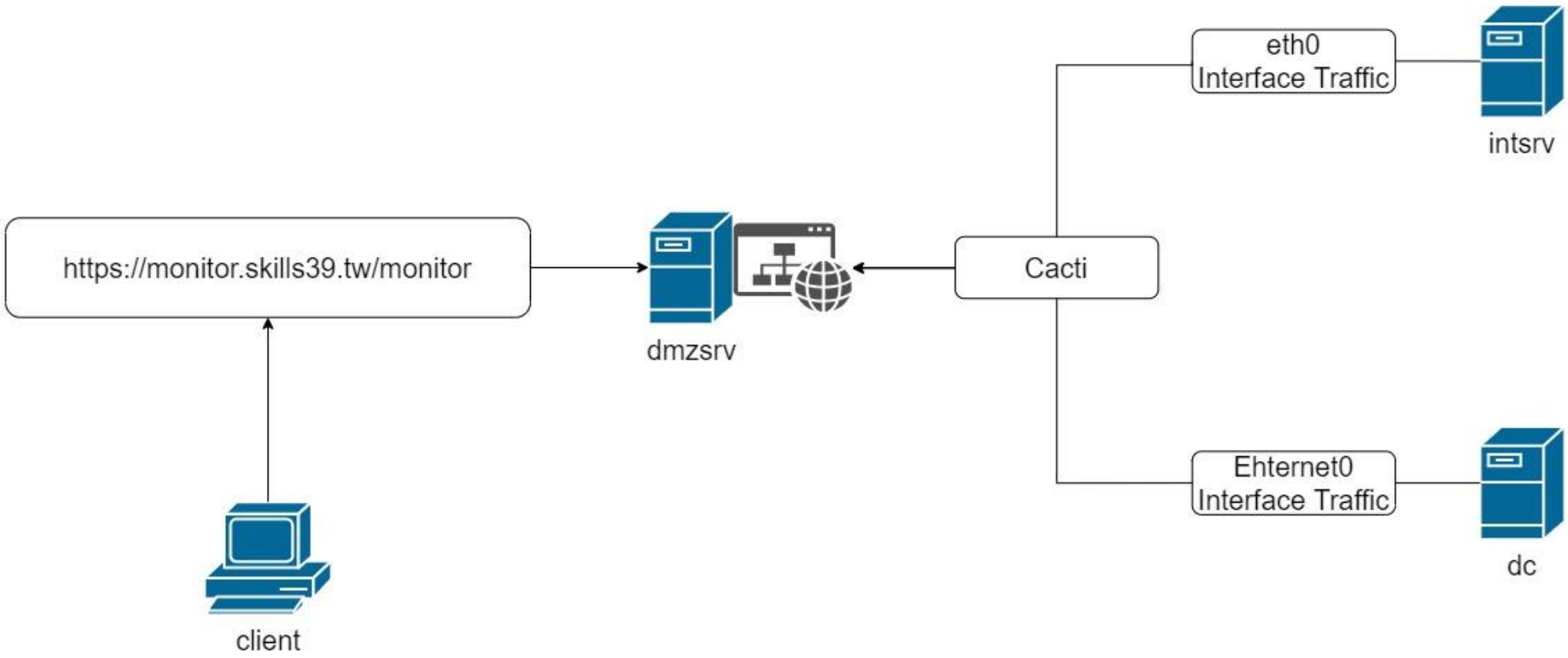
Default Hostname	OS	VMnet	IP Address	SSH User	SSH Password
node	Debian 11	VMnet15	192.168.1.2/24	root	Skills39

GRE over IPsec



Monitor


SNMP get operations
SNMP Agent
UDP 161
intsrv
SNMP
GET
SNMP
Community
pulibc
dmzsrv
SNMP Agent
UDP 161
dc


eth0
Interface Traffic
intsrv
https://monitor.skills39.tw/monitor
dmzsrv
Cacti
Ehternet0
Interface Traffic
dc
client